STAT

ARTICLE APPEARED
ON PAGE 2-A

WASHINGTON TIMES
18 March 1987

White House accused of 'cave-in' on security

By Bill Gertz
THE WASHINGTON TIMES

The White House was accused by intelligence officials yesterday of jeopardizing national security by "capitulating" to congressional pressure on a program for protecting sensitive, but unclassified, technical material.

One administration official, who declined to be identified, said recent White House actions on the subject have amounted to sinking what had been the "flagship" of President Reagan's six-year security program.

The controversy came into public view yesterday at a hearing before the House government operations subcommittee on legislation and national security, at which former national security adviser John M. Poindexter again refused to testify, invoking his Fifth Amendment rights.

The committee is trying to determine whether presidential security directives have placed undue restrictions on public access to scientific and technical information. The committee also is conducting hearings on the proposed Computer Security Act of 1987.

According to a letter made public during yesterday's session, Rear Adm. Poindexter's replacement, Frank Carlucci, has begun modifying a 1984 executive order on computer and communications security, and has lifted a policy directive aimed at protecting sensitive, but unclassified, technical information.

"[White House Chief of Staff Howard] Baker and Carlucci totally capitulated to the subcommittee's demands," the administration official said. "The cave-in was craven, but we'll probably see a lot more before it's over."

The official also blasted the White House for not invoking executive privilege to keep former national security officials from being questioned by the committee on sensitive intelligence issues.

Kenneth de Graffenreid, a former NSC intelligence adviser, testified that the administration's past security policies had curbed Soviet electronic spying.

"I think that the president's original directive and the policy which grew out of it ... were correct, proper and appropriate," Mr. de Graffenreid said in an interview. "I think it's unfortunate that the situation that we find ourselves in has resulted in the withdrawal of a statement that I believe is defensible."

According to subcommittee Chairman Jack Brooks, Texas Democrat, the law being considered is designed to secure sensitive information in federal computer systems without restricting public access to unclassified information.

In a Jan. 16 letter to Mr. Brooks, Mr. Baker wrote that Mr. Carlucci "has moved promptly to rescind the policy directive which you had cited as troublesome."

In a separate letter to Mr. Brooks, Mr. Carlucci said the NSC staff was reviewing a 1984 executive order, identified as National Security Decision Directive 145, "with an objective of finding a mechanism for eliminating the president's national security adviser from an implementation role with respect to this N.S.D.D."

Mr. Brooks charged that the policy "gave the national security agencies the authority to control public access to unclassified information located in civilian agencies and even the private sector."

"In effect, this gave DOD and the intelligence community 'Big Brother' control over all computer systems in the country," Mr. Brooks said.

Officials said Mr. Carlucci and Mr. Baker ignored advice from several administration legal advisers in not invoking executive privilege for Adm. Poindexter and Mr. de Graffenreid, thus forcing them to appear before the committee. They declined to testify voluntarily last month.

Mr. de Graffenreid testified that computer and communications security programs were a response to Soviet electronic spying on U.S. government information systems that he said were major targets of the KGB and other intelligence services.

"The KGB effort is massive, of increasing sophistication, and directed at us all around the world and at home within the United States," Mr. de Graffenreid said. "These activities, on the part of hostile intelligence services in the area of penetrating our secure communications and our computers, do palpable damage to the United States."

Contrary to charges made by Mr. Brooks, Mr. de Graffenreid said N.S.D.D. 145 was "machine-oriented" and "in no way restricts the legitimate access to information contained in communications or computer equipment."

"[It] is intended solely — and I would emphasize that — to prevent its interception or theft by hostile intelligence services," Mr. de Graffenreid said.